UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/936,415	02/01/2002	Ahmet Mursit Eskicioglu	RCA 89462	3679

7590 10/18/2005

Joseph S Tripoli
Thomson Multimedia Licensing Inc
PO Box 5312
Princeton, NJ 08543-5312

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/936,415	**Applicant(s)** ESKICIOGLU ET AL.	
	Examiner Longbit Chai	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 25 August 2000.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-20 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-20 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 01 February 2002 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 16 have been presented for examination. Claims 1, 4 – 10, 12, 15 have been amended; and new claims 17 – 20 have been added in an amendment filed 8/25/2005.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1, 2, 5, 8 and 14 are rejected under 35 U.S.C. 102(e) as being anticipated by Tsuria (PN: 6178242).

As per claim 1, Tsuria teaches a method for managing access, within a network comprising a first device interconnected to a second device, the method comprising:

(a) receiving said scrambled program in said first device, said scrambled program comprising a scrambled data component and a descrambling key (Tsuria: Column 3 Line 1 – 8 and Figure 1: the first device is interpreted as the IRD (Integrated Receiver Decoder) on Figure 1 / Element 110 and the second device is interpreted as the playback device (or VCR) on Figure 1 / Element 130 capable to present data for display on the monitor);

(b) rebundling, in said first device, said descrambling key using a unique key associated with said first device (Tsuria: Column 3 Line 1 – 8 and Column 8 Line 53 – 55);

(c) receiving, in said second device, said scrambled data component and said rebundled descrambling key (Tsuria: Column 9 Line 30 – 36);

(d) obtaining in said second device said descrambling key from said rebundled descrambling key (Tsuria: Column 10 Line 21 – 26); and

(e) descrambling, in said second device, said scrambled data component using said descrambling key (Tsuria: Column 10 Line 36 – 40).

As per claim 2, Tsuria teaches (a) decrypting said encrypted descrambling key using a key associated with said scrambled program; and (b) re-encrypting said descrambling key using said unique key associated with said first device to produce said rebundled descrambling key (Tsuria: Column 10 Line 36 – 40).

As per claim 5, Tsuria further teaches initializing said first device within said network (Tsuria: Column 8 Line 29 – 43 & Figure 1: the first device is IRD (Integrated Recording Decoder) which directly interfaces with the SDDS broadcasting system to discourage unauthorized duplication and subsequent play-back / recording).

As per claim 8, Tsuria teaches said descrambling key is one of encrypted using a private means if said scrambled program is received from prerecorded media or protected by a private means if said scrambled program is received from a service provider (Tsuria: Column 7 Line 50 – 57).

As per claim 14, Tsuria further teaches the first device is an access device and wherein the second device is a presentation device (Tsuria: Figure 1: the first device is interpreted as the IRD (Integrated Receiver Decoder) on Figure 1 / Element 110 and the second device is interpreted as the playback device (or VCR) on Figure 1 / Element 130 capable to present data for display on the monitor).

3. Claims 9 is rejected under 35 U.S.C. 102(e) as being anticipated by Wasilewski et al. (PN: 5870474).

As per claim 9, Wasilewski teaches a presentation device for managing access to a scrambled program comprising:

(a) means for receiving, from a first device coupled to the presentation device via a local network, said scrambled program comprising a scrambled data component and a rebundled descrambling key encrypted using a key associated with the local network (Wasilewski: Column 10 Line 9 – 12 and Column 31 – 33);

(b) a module for decrypting, in said presentation device, said rebundled descrambling key to generate said descrambling key (Wasilewski: Column 10 Line 9 – 12 and Column 31 – 33);

(c) a module for descrambling, in said presentation device, said scrambled data component using said descrambling key to obtain a descrambled program (Wasilewski: Column 9 Line 47 – 48); and

(d) means for presenting said descrambled program (Wasilewski: Column 9 Line 47 – 48).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 3, 6 – 7, 10, 12 – 13, 17 – 18 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsuria (PN: 6178242), in view of Wasilewski et al. (PN: 5870474).

As per claim 10, Tsuria teaches a method for managing access to a scrambled program received from a service provider within a network having an access device and a presentation device, said method comprising:

(a) receiving said scrambled program in an access device, said scrambled program comprising a scrambled data component and an encrypted descrambling key (Tsuria: Column 3 Line 1 – 8 and Figure 1: the access device is interpreted as the IRD (Integrated Receiver Decoder) on Figure 1 / Element 110 and the presentation device is interpreted as the playback device (or VCR) on Figure 1 / Element 130 capable to present data for display on the monitor);

(b) decrypting, in said access device, said encrypted descrambling key using a key associated with said service provider (Tsuria: Column 3 Line 1 – 8 and Column 3 Line 11 – 16);

(d) receiving, in said presentation device, said scrambled data-component and said re-encrypted descrambling key (Tsuria: Column 10 Line 21 – 40);

(e) decrypting, in said presentation device, said re-encrypted descrambling key to obtain said descrambling key (Tsuria: Column 10 Line 21 – 40); and

(f) descrambling, in said presentation device, said scrambled data component using said descrambling key (Tsuria: Column 10 Line 21 – 40);

(c) re-encrypting said descrambling key, in said access device, using a public key associated with said access device (Tsuria: Column 3 Line 1 – 8 and Column 8 Line 53 – 55). However, Tsuria teaches re-encrypting said descrambling key in said access device but does not disclose expressly using a public key.

Wasilewski teaches using the public key as the higher-level encryption key to protect the lower-level encryption key over a communication network to the receiving terminal module (Wasilewski: Column 3 Line 53 – 67).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Wasilewski within the system of Tsuria because (a) Tsuria teaches producing and recording digital data stream, and particularly for protecting recorded digital data stream (Tsuria: Column 1 Line 60 – 63) and (b) Wasilewski teaches a control system for providing secure transmission of recording digital data stream (such as "movie on demand") between a service provider and a customer's set top box over a digital network (Wasilewski: Column 1 Line 15 – 25).

As per claim 3, Tsuria does not disclose expressly said unique key associated with said first device is a public key, said public key being located in said first device and a corresponding private key being located in said second device.

Wasilewski teaches said unique key associated with said first device is a public key, said public key being located in said first device and a corresponding private key being located in said second device (Wasilewski: Column 3 Line 62 – 67). Same rationale of combination applies here as above in rejecting the claim 10.

As per claim 6, Tsuria does not disclose expressly initializing comprises the step of receiving a public key from a conditional access provider.

Wasilewski teaches initializing comprises the step of receiving a public key from a conditional access provider (Wasilewski: Column 3 Line 53 – 67 and Column 7 Line 38 – 43). Same rationale of combination applies herein as above in rejecting the claim 10.

Accordingly, Tsuria as modified teaches:

the step of initializing comprises the step of receiving said public key from a conditional access provider (Wasilewski: Column 3 Line 53 – 67 and Column 7 Line 38 – 43), said step of receiving comprising authentication of said conditional access provider (Wasilewski: Column 11 Line 4 – 5; Tsuria: Column 8 Line 30 – 31).

As per claim 7, Tsuria teaches a re-encryption key is pre-stored in a smart card coupled to said first device or in said first device (Tsuria: Column 8 Line 30 – 31). However, Tsuria does not disclose expressly a re-encryption key is a public key.

Wasilewski teaches a re-encryption key is a public key (Wasilewski: Column 3 Line 53 – 67). Same rationale of combination applies here as above in rejecting the claim 10.

Accordingly, Tsuria as modified teaches:

a public key is pre-stored in a smart card coupled to said first device or in said first device.

As per claim 11, Tsuria as modified teaches said scrambled program is prerecorded on media and provided to said access device, said encrypted descrambling key being received from said prerecorded media (Tsuria: Column 3 Line 37 – 39).

As per claim 12, the claim limitations are met as the same reasons as that set forth in the paragraph above regarding to claim 10 with the exception of the feature recording said scrambled data component and said re-encrypted descrambling key on media coupled to said recording device, and providing said scrambled data component and said re-encrypted descrambling key to a presentation device. However, Tsuria teaches recording said scrambled data component and said re-encrypted descrambling key on media coupled to said recording device (Tsuria: Column 3 Line 37 – 39), and providing said scrambled data component and said re-encrypted descrambling key to a presentation device (Tsuria: Column 9 Line 30 – 36).

As per claim 13, Tsuria teaches said scrambled program is prerecorded on media (Tsuria: Column 1 Line 60 – 9).

As per claim 17, Tsuria teaches an access device, comprising:

a signal input for receiving a scrambled program from a service provider, the scrambled program including a scrambled data component and an encrypted descrambling key (Wasil'474: Column 8 Line 65 – 66);

a decrypting unit for obtaining the descrambling key using a key associated with the scrambled program (Tsuria: Column 3 Line 1 – 8 and Figure 1: the access device is interpreted as the IRD (Integrated Receiver Decoder) on Figure 1 / Element 110 and the presentation device is interpreted as the playback device (or VCR) on Figure 1 / Element 130 capable to present data for display on the monitor);

an encryption unit for re-encrypting the descrambling key using a public key associated with the access device (Tsuria: Column 3 Line 1 – 8 and Column 8 Line 53 – 55). However, Tsuria teaches re-encrypting said descrambling key in said access device but does not disclose expressly using a public key.

Wasilewski teaches using the public key as the higher-level encryption key to protect the lower-level encryption key over a communication network to the receiving terminal module (Wasilewski: Column 3 Line 53 – 67).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Wasilewski within the system of Tsuria because (a) Tsuria teaches producing and recording digital data stream, and particularly for protecting recorded digital data stream (Tsuria: Column 1 Line 60 – 63) and (b) Wasilewski teaches a control system for providing secure transmission of recording digital data stream (such as "movie on demand") between a service provider and a customer's set top box over a digital network (Wasilewski: Column 1 Line 15 – 25).

Tsuria in view of Wasilewski teaches:

a signal output coupled to a digital bus for transmitting the scrambled data component and the re-encrypted descrambling key to a presentation device via the digital bus, wherein only a presentation device having a corresponding private key is able to decrypt the re-encrypted descrambling key and descramble the scrambled content (Wasilewski: Column 3 Line 62 – 65).

As per claim 18, Tsuria as modified teaches he public key is periodically received from a conditional access provider (Wasilewski: Column 7 Line 38 – 40 and Column 10 Line 4 – 12).

As per claim 20, Tsuria as modified teaches the signal output transmits identification data associated with the access device and copy control information along with the re-encrypted descrambling key (Wasilewski: Column 3 Line 65 – 67 and Column 7 Line 38 – 43: the networking packet must contain the identification data associated with the access device such as SRC / DEST address).

5. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tsuria (PN: 6178242), in view of Cohen et al. (PN: 5481609).

As per claim 4, Tsuria teaches the step of rebundling is performed within a first smart card coupled to said first device (Tsuria: Column 7 Line 1 – 9 and Column 6 Line 66 – Column 7 Line 1). Tsuria does not disclose expressly the steps of decrypting and descrambling are performed within a second smart card coupled to said second device.

Cohen teaches the steps of decrypting and descrambling are performed within a second smart card coupled to said second device (Cohen: Figure 3 Element 30 / 32 and Column 178 Line 21 – 23).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cohen within the system of Tsuria because (a) Tsuria teaches producing and recording digital data stream, and particularly for protecting recorded digital data stream (Tsuria: Column 1 Line 60 – 63) and (b) Cohen teaches enhancing security in a broadcast transmission system by containing a separate identification element which is sensible by a decoder in each executing apparatus (Cohen: Column 2 Line 1 – 3).

6. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al. (PN: 5870474), in view of Tsuria (PN: 6178242).

As per claim 11, Wasilewski does not disclose expressly said scrambled program is prerecorded on media and provided to said access device, said encrypted descrambling key being received from said prerecorded media.

Tsuria teaches said scrambled program is prerecorded on media and provided to said access device, said encrypted descrambling key being received from said prerecorded media (Tsuria: Column 3 Line 37 – 39).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Tsuria within the system of Wasilewski because Tsuria teaches providing an improved system for producing and recording digital data streams, and particularly for protecting recorded digital data streams (Tsuria: Column 1 Line 60 – 64).

7. Claims 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bando (PN: 5774548), in view of Kimura (PN: 6674858).

As per claim 15, Bando teaches a method for transforming :in a security device, content information contained in a scrambled program received from a service provider comprising:

receiving in said security device the scrambled program containing scrambled content information and a control word; and descrambling the scrambled content in the security device using the control word (Bando: Column 1 Line 33 – 40: Ks (scramble / descramble key associated with ECM is equivalent to control word of ECM);

Bando does not disclose expressly generating in the security device another scrambling key.

Kimura teaches generating in the security device another scrambling key; and re-scrambling the content using said another scrambling key (Kimura: Column 2 Line 23 – 26 & Figure 9 Element 21 / 29: a device key is used as a scrambling / descramble key).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Kimura within the system of Bando because Kimura teaches a digital broadcast system with effective copy protection specific process that the pay broadcast can be recorded only by the proper receiver (Kimura: Column 1 Line 38 – 42).

encrypting a local ECM containing the re-scrambled content using a unique key (Bando: Column 1 Line 50: the unique key = $K_{w,}$ which encrypts the scramble key K_s associated with local ECM).

As per claim 16, Bando further teaches determining user entitlement to the scrambled program prior to descrambling the scrambled content (Bando: Column 1 Line 44 – 51 and Column 1 Line 41 – 42).

8. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tsuria (PN: 6178242), in view of Wasilewski et al. (PN: 5870474), and in view of Smyers et al. (PN: 5948136).

As per claim 19, Wasilewski does not teach the signal output authenticates the presentation device before transmitting the scrambled data component and the re-encrypted descrambling key to the presentation device.

Smyers the signal output authenticates the presentation device before transmitting the scrambled data component and the re-encrypted descrambling key to the presentation device (Smyers: Column 4 Line 38 – 42).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Smyers within the system of Tsuria as modified because Smyers teaches providing hardware authentication mechanism to enhance communication securities between two devices.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC
LBC

Primary Examiner
AU2131
10/13/05